ELSEVIER

Available online at www.sciencedirect.com

ScienceDirect

Journal of Algebra 309 (2007) 282–291

JOURNAL OF Algebra

www.elsevier.com/locate/jalgebra

Hilbert's Fourteenth Problem and algebraic extensions

Shigeru Kuroda [1]

Research Institute for Mathematical Sciences, Kyoto University, Kyoto 606-8502, Japan

Received 12 April 2006

Communicated by Paul Roberts

Abstract

Let $k[X]$ be the polynomial ring in n variables over a field k for some $n \in \mathbf{N}$, and $k(X)$ its field of fractions. Assume that L is a subfield of $k(X)$ containing k over which $k(X)$ is algebraic. In spite of being an important issue in Hilbert's Fourteenth Problem, relations between finite generation of the k-subalgebra $L \cap k[X]$ of $k[X]$ and the extension degree $[k(X) : L]$ of $k(X)$ over L have not been investigated. In the present paper, we give an example of L with $[k(X) : L] = d$ such that $L \cap k[X]$ is not finitely generated for each $d \in \mathbf{N}$ with $d \geqslant 3$ for $n = 3$.

Keywords: Hilbert's Fourteenth Problem

1. Introduction

Let k be a field, $k[X] = k[X_1, \ldots, X_n]$ the polynomial ring in n variables over k for some $n \in \mathbf{N}$, and $k(X)$ the field of fractions of $k[X]$. Assume that L is a subfield of $k(X)$ containing k. Then, Hilbert's Fourteenth Problem asks whether the k-subalgebra $L \cap k[X]$ of $k[X]$ is finitely generated. Zariski [13] showed in 1954 that the answer to this problem is affirmative if the transcendence degree of L over k is at most two, while Nagata [9] gave the first counterexample in 1958 in the case where $n = 32$ and the transcendence degree of L over k is four. Nagata's result is valid for any field k which is not an algebraic extension of a finite field. In 1990, Roberts [11] constructed a different type of counterexample in which $n = 7$ and the transcendence degree of

E-mail address: kuroda@kurims.kyoto-u.ac.jp.

[1] Partly supported by the Grant-in-Aid for JSPS Fellows, The Ministry of Education, Science, Sports and Culture, Japan.

0021-8693/$ – see front matter
doi:10.1016/j.jalgebra.2006.10.008

L over k is six, where k is a field of characteristic zero. Following Nagata and Roberts, several new counterexamples have been constructed. Mukai [8] and Steinberg [12] refined Nagata's construction. Kojima–Miyanishi [3] and the author [4] generalized Roberts' counterexample in higher dimensions, while Freudenburg [2], Daigle–Freudenburg [1] and the author [5] improved Roberts' construction to obtain counterexamples in lower dimensions. All of these counterexamples involve the invariant rings of certain algebraic group actions or the kernels of derivations, where $k(X)$ is transcendental over L. On the other hand, Noether's classical result [10] implies that the answer to Hilbert's Fourteenth Problem is affirmative if L is the field of fractions of the invariant ring of a finite group action on $k[X]$. In this case, $k(X)$ is algebraic over L. However, Hilbert's Fourteenth Problem has not been studied well in the general case where $k(X)$ is algebraic over L. It was unknown whether there could exist a counterexample L with $k(X)$ algebraic over L until the author [6] gave one for $n = 3$. Here, we note that $k(X)$ is necessarily algebraic over L if $n = 3$ and $L \cap k[X]$ is not finitely generated due to Zariski [13].

The purpose of this paper is to investigate the relation between finite generation of $L \cap k[X]$ and the structure of the extension $k(X)$ over L. Since the field $k(X)$ is finitely generated, the extension degree $[k(X) : L]$ is finite if and only if $k(X)$ is algebraic over L. For the counterexamples in [6], $[k(X) : L]$ can only be certain even numbers at least twenty-two, as will be explained at the end of Section 5. In the present paper, we construct counterexamples for $n = 3$ by a much simpler method than that in [6]. As a consequence of our main result, we obtain a counterexample L such that $[k(X) : L] = d$ for each $d \in \mathbf{N}$ with $d \geqslant 3$.

Assume that $n = 3$ and the characteristic of k is zero. Let δ_1 and δ_2 be natural numbers with $\delta_1 < \delta_2$ such that δ_2 is not divisible by δ_1, and δ_0 the greatest common divisor of δ_1 and δ_2. We set $\delta'_0 = \delta_1\delta_2/\delta_0$ and $\delta'_i = \delta_i/\delta_0$ for $i = 1, 2$. Let π_1 and π_2 be polynomials in a variable z over k whose constant terms are 1 such that the radical of the ideal $(\alpha_1\pi_1^{\delta'_2} + \alpha_2\pi_2^{\delta'_1})\bar{k}[z]$ does not contain π_1 or π_2 for any $\alpha_1, \alpha_2 \in \bar{k}$, where $\bar{k}$ is an algebraic closure of k. Then, the maximal integer ϵ' for which $\pi_1^{\delta'_2} - \pi_2^{\delta'_1}$ is contained in $z^{\epsilon'}k[z]$ is positive. So, we may find $\epsilon \in \mathbf{Z}$ such that $\epsilon\epsilon' \geqslant \delta'_0 + 1$ and $\epsilon \geqslant \delta_0$. For $\Delta = (\delta_1, \delta_2; \pi_1, \pi_2)$ and ϵ as above, we define L^{ϵ}_{Δ} to be the subfield of $k(X)$ generated by $\Pi_0 := X_2^{-\delta_0} + X_3$ and $\Pi_i := X_2^{-\delta_i}\pi_i(X_1X_2^{\epsilon})$ for $i = 1, 2$ over k. Here, for a commutative algebra R, $\phi \in R[z]$ and $f \in R$, we denote by $\phi(f)$ the element of R obtained from ϕ by substituting f for z.

Here is our main result.

Theorem 1.1. *The k-subalgebra $L^{\epsilon}_{\Delta} \cap k[X]$ of $k[X]$ is not finitely generated.*

Let M_{Δ} be the subfield of $k(X)'$ generated by $X_2^{\delta_i}\pi_i(X_1X_2^{-1})$ for $i = 1, 2$ over k, where $k(X)' = k(X_1, X_2)$. Then, L^{ϵ}_{Δ} is isomorphic to $M_{\Delta}(X_3)$ via the automorphism of $k(X)$ over k defined by $X_1 \mapsto X_1X_2^{\epsilon-1}$, $X_2 \mapsto X_2^{-1}$ and $X_3 \mapsto -X_2^{\delta_0} + X_3$. So, we get the following.

Proposition 1.2. *The automorphism group of $k(X)$ over L^{ϵ}_{Δ} is isomorphic to that of $k(X)'$ over M_{Δ}, $[k(X) : L^{\epsilon}_{\Delta}] = [k(X)' : M_{\Delta}]$, and $k(X)/L^{\epsilon}_{\Delta}$ is a Galois extension if and only if $k(X)'/M_{\Delta}$ is a Galois extension.*

In fact, if M is a subfield of $k(X)'$, then the automorphism group of $k(X)$ over $M(X_3)$ is isomorphic to that of $k(X)'$ over M, $[k(X) : M(X_3)] = [k(X)' : M]$, and $k(X)/M(X_3)$ is a Galois extension if and only if $k(X)'/M$ is a Galois extension.

For example, let $\pi_i = 1 + (-1)^i z$ for $i = 1, 2$. Then, π_1 and π_2 are mutually prime, and $\alpha_1 \pi_1^{\delta_2'} + \alpha_2 \pi_2^{\delta_1'}$ is not contained in $\bar{k} \setminus \{0\}$ for any $\alpha_1, \alpha_2 \in \bar{k}$, since $\delta_1' < \delta_2'$ by assumption. So, the radical of $(\alpha_1 \pi_1^{\delta_2'} + \alpha_2 \pi_2^{\delta_1'})\bar{k}[z]$ does not contain the greatest common divisor of π_1 and π_2, and hence does not contain π_1 or π_2 for any $\alpha_1, \alpha_2 \in \bar{k}$. In this case, $\epsilon' = 1$ independently of the choice of δ_1 and δ_2. Hence, ϵ is an integer at least $\delta_0' + 1$, and L_Δ^ϵ is the subfield of $k(X)$ generated by $X_2^{-\delta_0} + X_3$ and $X_2^{-\delta_i}(1 + (-1)^i X_1 X_2^\epsilon)$ for $i = 1, 2$ over k. Let us show that $[k(X) : L_\Delta^\epsilon] = \delta_2$. By definition, M_Δ is generated by $\Pi_i' := X_2^{\delta_i} + (-1)^i X_1 X_2^{\delta_i - 1}$ for $i = 1, 2$. Observe that $k(X)'$ is generated by X_2 over M_Δ, and $\Psi(X_2) = 0$ for $\Psi = 2z^{\delta_2} - \Pi_1' z^{\delta_2 - \delta_1} - \Pi_2'$. Since Π_1' and Π_2' are algebraically independent over k, it easily follows that Ψ is irreducible over M_Δ. Indeed, Ψ is irreducible over the unique factorization domain $k[\Pi_1', \Pi_2'/\Pi_1']$ by the Eisenstein criterion for irreducibility. Hence, $[k(X)' : M_\Delta] = \delta_2$. Thus, we get $[k(X) : L_\Delta^\epsilon] = \delta_2$ by Proposition 1.2. Note that, for each $\delta_2 \in \mathbf{N}$ with $\delta_2 \geqslant 3$, there exists $\delta_1 \in \mathbf{N}$ with $\delta_1 < \delta_2$ such that δ_2 is not divisible by δ_1. Therefore, we obtain the following corollary to Theorem 1.1.

Corollary 1.3. *Assume that $n = 3$ and k is an arbitrary field of characteristic zero. Then, for each $d \in \mathbf{N}$ with $d \geqslant 3$, there exists a subfield L of $k(X)$ containing k such that $[k(X) : L] = d$ and $L \cap k[X]$ is not finitely generated.*

In Section 5, we show that $k(X)/L_\Delta^\epsilon$ is not a Galois extension for this Δ. However, $k(X)/L_\Delta^\epsilon$ can be a Galois extension for suitable k and Δ. For instance, assume that k contains a primitive δ_ith root ζ_i of unity and $\pi_i = (1 + (-1)^i z)^{\delta_i}$ for $i = 1, 2$. In this case, M_Δ is generated by $(X_2 + (-1)^i X_1)^{\delta_i}$ for $i = 1, 2$. We define an automorphism τ_i of $k(X)'$ over k by

$$\tau_i\big(X_2 + (-1)^i X_1\big) = \zeta_i\big(X_2 + (-1)^i X_1\big) \quad \text{and} \quad \tau_i\big(X_2 - (-1)^i X_1\big) = X_2 - (-1)^i X_1$$

for $i = 1, 2$, and G to be the subgroup of the automorphism group of $k(X)'$ generated by τ_1 and τ_2. Then, we see easily that the invariant subfield of $k(X)'$ for G is equal to M_Δ. Hence, $k(X)'/M_\Delta$ is a Galois extension with Galois group G. Thus, $k(X)/L_\Delta^\epsilon$ is a Galois extension whose Galois group is isomorphic to G by Proposition 1.2. We remark that the order of τ_i is equal to δ_i for $i = 1, 2$, and G is isomorphic to $(\mathbf{Z}/\delta_1\mathbf{Z}) \times (\mathbf{Z}/\delta_2\mathbf{Z})$.

We note that the author [7] recently constructed a counterexample L with $[k(X) : L] = 2$ when $n \geqslant 4$. In fact, he gave a faithful action of G on $k(X)$ such that $k(X)^G \cap k[X]$ is not finitely generated for each finite group $G \neq \{1\}$. Here, k is an arbitrary field of characteristic zero, and n is any natural number with $n \geqslant 4$ if the order of G is two, and $n \geqslant m(G) + 1$ otherwise, where $m(G)$ is the minimal natural number for which G acts on the set $\{1, 2, \ldots, m(G)\}$ faithfully and transitively. However, the case where $n = 3$ and $[k(X) : L] = 2$ remains open for any k.

Problem 1.4. Assume that $n = 3$. Let L be a subfield of $k(X)$ containing k such that $[k(X) : L] = 2$. Is the k-subalgebra $L \cap k[X]$ of $k[X]$ always finitely generated?

The following problem is also unsettled.

Problem 1.5. Assume that $n = 3$ and $k = \mathbf{Q}$. Let L be a subfield of $k(X)$ containing k such that $k(X)/L$ is a Galois extension. Is the k-subalgebra $L \cap k[X]$ of $k[X]$ always finitely generated?

2. Infinite generation

The following lemma is useful in proving that a k-subalgebra of $k[X]$ is not finitely generated.

Lemma 2.1. *A k-subalgebra A of $k[X]$ is not finitely generated if the following conditions hold*:

(i) *No polynomial in which the monomial X_n^l appears with nonzero coefficient is contained in A for any $l \in \mathbf{N}$.*
(ii) *There exists $g \in k[X] \setminus k$ such that A contains a polynomial of the form $gX_n^l + (\text{terms of lower degree in } X_n)$ for each $l \in \mathbf{N}$.*

Proof. Let S be the set of $(a_1, \dots, a_n)$ for $a_1, \dots, a_n \in \mathbf{Z}_{\geqslant 0}$ such that $X_1^{a_1} \cdots X_n^{a_n}$ appears in some element of A, and $\tilde{S}$ the subsemigroup of $(\mathbf{Z}_{\geqslant 0})^n$ generated by S, where $\mathbf{Z}_{\geqslant 0}$ denotes the set of nonnegative integers. By the condition (i), $S \setminus \{0\}$ does not contain an element whose first $n-1$ components are zero. Hence, $\tilde{S} \setminus \{0\}$ also does not contain such elements. We define a function $N : \tilde{S} \setminus \{0\} \to \mathbf{R}$ by $N(a) = (\sum_{i=1}^{n-1} a_i)^{-1} a_n$ for $a = (a_1, \dots, a_n)$. Suppose to the contrary that A is finitely generated. Then, we may find a finite subset S' of S such that the k-vector space generated by $X_1^{a_1} \cdots X_n^{a_n}$ for $a_1, \dots, a_n \in \mathbf{Z}_{\geqslant 0}$ with $(a_1, \dots, a_n) \in S'$ contains a generating set for A. Let M be the maximum among $N(a)$ for $a \in S' \setminus \{0\}$. Then, $N(a) \leqslant M$ for each $a \in S \setminus \{0\}$. Actually, the semigroup $\tilde{S}$ is generated by S', and $N(a+b) \leqslant \max\{N(a), N(b)\}$ for $a, b \in \tilde{S} \setminus \{0\}$. Assume that the monomial $X_1^{b_1} \cdots X_n^{b_n}$ appears in g for some $b_1, \dots, b_n \in \mathbf{Z}_{\geqslant 0}$. Then, S contains $b(l) := (b_1, \dots, b_n + l)$ for each $l \in \mathbf{Z}_{\geqslant 0}$ by the condition (ii). However, $N(b(l)) > M$ for sufficiently large l. This is a contradiction. Therefore, A is not finitely generated. □

In Sections 3 and 4, we will prove the following propositions.

Proposition 2.2. *No polynomial in which the monomial X_3^l appears with nonzero coefficient is contained in $L_\Delta^\epsilon \cap k[X]$ for any $l \in \mathbf{N}$.*

Proposition 2.3. *There exists $\phi \in k[X] \setminus k$ such that $L_\Delta^\epsilon \cap k[X]$ contains a polynomial of the form $\phi X_3^l + (\text{terms of lower degree in } X_3)$ for each $l \in \mathbf{N}$.*

With the aid of Lemma 2.1, Theorem 1.1 immediately follows from these propositions.

3. The structure of $k(\Pi_1, \Pi_2)$

Let $k[X, X^{-1}]$ denote the Laurent polynomial ring in X_1, X_2 and X_3 over k, and $k[\Pi] = k[\Pi_0, \Pi_1, \Pi_2]$. For each $i \in \mathbf{Z}$, we denote by V_i the k-vector space generated by $X_1^{i_1} X_2^{i_2} X_3^{i_3}$ for $i_1, i_2, i_3 \in \mathbf{Z}$ with $\epsilon i_1 - i_2 + \delta_0 i_3 = i$. Then, $k[X, X^{-1}]$ is equal to the direct sum of the k-vector spaces V_i for $i \in \mathbf{Z}$, and $V_i V_j$ is contained in V_{i+j} for each $i, j \in \mathbf{Z}$. Hence, a $\mathbf{Z}$-grading is defined on $k[X, X^{-1}]$. Since $X_2^{-\delta_i}$, X_3 and $X_1 X_2^\epsilon$ are contained in V_{δ_i}, V_{δ_0} and V_0, respectively, we see that Π_i is contained in V_{δ_i} for each i. Hence, $k[\Pi]$ is graded by this $\mathbf{Z}$-grading. It follows that f is in $k[X]$ if and only if each $\mathbf{Z}$-homogeneous component of f is in $k[X]$ for $f \in k[X, X^{-1}]$. Thus, $k[\Pi] \cap k[X]$ is also graded by this $\mathbf{Z}$-grading.

Assume that g is an element of $k[\Pi_1, \Pi_2] \cap V_l$ for some $l \in \mathbf{Z}$. Then, $g \neq 0$ only if $l \geqslant 0$. If this is the case, then we may write

$$g = \Pi_1^{a_1} \Pi_2^{a_0 \delta_1' + a_2} \sum_{i=0}^{a_0} \lambda_{a_0 - i} \left(\Pi_1^{\delta_2'} \Pi_2^{-\delta_1'} \right)^i, \tag{3.1}$$

where $a_0, a_1, a_2 \in \mathbf{Z}_{\geqslant 0}$ with $a_0\delta'_0 + \sum_{i=1}^{2} a_i\delta_i = l$, and $\lambda_i \in k$ for $i = 0, \ldots, a_0$ with $\lambda_i \neq 0$ for $i = 0, a_0$. Let $\mu_1, \ldots, \mu_{a_0}$ be the solutions of the equation $\sum_{i=0}^{a_0} \lambda_{a_0-i} z^i = 0$ in $\bar{k}$. Then, $\mu_i \neq 0$ for each i, and (3.1) is expressed as

$$g = \lambda_0 \Pi_1^{a_1} \Pi_2^{a_2} \prod_{i=1}^{a_0} \bigl(\Pi_1^{\delta'_2} - \mu_i \Pi_2^{\delta'_1}\bigr). \tag{3.2}$$

Lemma 3.1. *The k-algebra $k(\Pi_1, \Pi_2) \cap k[X][X_2^{-1}]$ is contained in $k[\Pi_1, \Pi_2]$.*

Proof. Take any $f \in k(\Pi_1, \Pi_2) \cap k[X][X_2^{-1}] \setminus \{0\}$. Then, there exist $f_1, f_2 \in k[\Pi_1, \Pi_2] \setminus \{0\}$ such that $f = f_1/f_2$. Let $\bar{f}$, $\bar{f}_1$ and $\bar{f}_2$ respectively be the nonzero $\mathbf{Z}$-homogeneous components of f, f_1 and f_2 of the highest degree. Then, $\bar{f}\bar{f}_2 = \bar{f}_1$, since $ff_2 = f_1$. In addition, $\bar{f}$ is in $k[X][X_2^{-1}]$, while $\bar{f}_1$ and $\bar{f}_2$ are in $k[\Pi_1, \Pi_2]$. Thus, $\bar{f}$ is also in $k(\Pi_1, \Pi_2) \cap k[X][X_2^{-1}]$. Therefore, it suffices to show that $\bar{f}$ is contained in $k[\Pi_1, \Pi_2]$. Since $\bar{f}_1$ and $\bar{f}_2$ are $\mathbf{Z}$-homogeneous, they are expressed as in the right-hand side of (3.2). Hence, we may write

$$\bar{f} = \alpha \Pi_1^{b_{s+1}} \Pi_2^{b_{s+2}} \prod_{i=1}^{s} \bigl(\Pi_1^{\delta'_2} - \gamma_i \Pi_2^{\delta'_1}\bigr)^{b_i}, \tag{3.3}$$

where $s \in \mathbf{Z}_{\geqslant 0}$, $b_1, \ldots, b_{s+2} \in \mathbf{Z}$ with $(\sum_{i=1}^{s} b_i)\delta'_0 + \sum_{i=1}^{2} b_{s+i}\delta_i = l$, $\alpha \in k \setminus \{0\}$, and $\gamma_1, \ldots, \gamma_s \in \bar{k} \setminus \{0\}$ with $\gamma_i \neq \gamma_j$ if $i \neq j$.

We show that $b_1, \ldots, b_{s+2}$ are nonnegative. Put $g_i = \pi_1^{\delta'_2} - \gamma_i \pi_2^{\delta'_1}$ for $i = 1, \ldots, s$ and $g_{s+i} = \pi_i$ for $i = 1, 2$, and define $h_j = \prod_{i \in I_j} g_i (X_1 X_2^{\epsilon})^{b_i}$ for $j = 0, 1$, where I_0 and I_1 are the sets of i such that $b_i \geqslant 0$ and $b_i < 0$, respectively. Then, we have $\bar{f} = \alpha X_2^{-l} h_0 h_1$. By assumption, $\bar{f}$ is contained in $\bar{k}(X_2)[X_1]$, while h_0 and h_1^{-1} are contained in $\bar{k}[X_1, X_2]$. Hence, h_0 is divisible by h_1^{-1} in $\bar{k}(X_2)[X_1]$. Now, suppose to the contrary that $b_p < 0$ for some p. Then, $g_p(X_1 X_2^{\epsilon})$ divides h_1^{-1}, and so divides h_0. Note that g_p is not contained in $\bar{k} \setminus \{0\}$. In fact, the radical of $g_p\bar{k}[z]$ does not contain π_1 or π_2 by assumption. Hence, $g_p(\beta) = 0$ for some $\beta \in \bar{k}$. Then, $X_1 X_2^{\epsilon} - \beta$ divides h_0, and so divides $g_q(X_1 X_2^{\epsilon})$ for some $q \in I_0$. Then, $g_q(\beta) = 0$. Since $p \neq q$, we have $\pi_i(\beta) = 0$ for $i = 1, 2$. Since this holds for each $\beta \in \bar{k}$ with $g_p(\beta) = 0$, the radical of $g_p\bar{k}[z]$ contains π_1 and π_2. This is a contradiction. Therefore, $b_1, \ldots, b_{s+2}$ are nonnegative, and thus $\bar{f}$ is contained in $k[\Pi_1, \Pi_2]$. □

Using Lemma 3.1, we get the following.

Proposition 3.2. *The k-algebra $L_{\Delta}^{\epsilon} \cap k[X]$ is contained in $k[\Pi]$.*

Proof. First, we show that $L_{\Delta}^{\epsilon} \cap k(X)'[X_3]$ is contained in $k(\Pi_1, \Pi_2)[\Pi_0]$. Take any $G \in L_{\Delta}^{\epsilon} \cap k(X)'[X_3]$. Then, there exist $g_1, g_2 \in k(\Pi_1, \Pi_2)[z]$ such that $G = g_1(\Pi_0)/g_2(\Pi_0)$. Suppose that G is not contained in $k(\Pi_1, \Pi_2)[\Pi_0]$. Then, g_1 is not divisible by g_2. By replacing g_1 with its remainder divided by g_2, we may assume that the degree of g_1 is less than that of g_2. Then, $g_i(\Pi_0)$ is in $k(X)'[X_3]$ for $i = 1, 2$, and the degree of $g_1(\Pi_0)$ in X_3 is less than that of $g_2(\Pi_0)$, since $\Pi_0 = X_2^{-\delta_0} + X_3$. This contradicts that G is contained in $k(X)'[X_3]$. Therefore, $L_{\Delta}^{\epsilon} \cap k(X)'[X_3]$ is contained in $k(\Pi_1, \Pi_2)[\Pi_0]$.

Now, take any $F \in L_{\Delta}^{\epsilon} \cap k[X]$. Since F is a polynomial in X_3 over $k[X_1, X_2]$ and $X_3 = \Pi_0 - X_2^{-\delta_0}$, we may write $F = \sum_{i=0}^{l} \phi_i \Pi_0^{l-i}$, where $l \in \mathbf{Z}_{\geqslant 0}$ and $\phi_i \in k[X_1, X_2, X_2^{-1}]$ for each i. On the other hand, F is contained in $k(\Pi_1, \Pi_2)[\Pi_0]$ by the argument above. Hence, we may write $F = \sum_{i=0}^{l'} \phi_i' \Pi_0^{l'-i}$, where $l' \in \mathbf{Z}_{\geqslant 0}$ and $\phi_i' \in k(\Pi_1, \Pi_2)$ for each i. Since Π_0 is transcendental over $k(X)'$, it follows that $l = l'$ and $\phi_i = \phi_i'$ for each i. Thus, ϕ_i is contained in $k(\Pi_1, \Pi_2) \cap k[X_1, X_2, X_2^{-1}]$, and hence contained in $k[\Pi_1, \Pi_2]$ for each i by Lemma 3.1. Therefore, F is contained in $k[\Pi]$. □

To prove Propositions 2.2 and 2.3, we make use of Taylor's formula. Let $\phi = (\phi_i)_{i=0}^{l}$ be an element of $k(X)^{l+1}$ for some $l \in \mathbf{Z}_{\geqslant 0}$. For $m = 0, \ldots, l$, we define a map $F_m^{\phi} : k(X) \to k(X)$ by

$$F_m^{\phi}(f) = \sum_{i=0}^{l-m} \frac{\phi_{l-m-i}}{i!} f^i$$

for $f \in k(X)$. Note that $F_m^{\phi}(f)$ is the mth order derivative of $F_0^{\phi}(f)$ in f, where we regard f as an indeterminate over $k(X)$. Hence, by Taylor's formula, it follows that

$$F_0^{\phi}(f+g) = \sum_{i=0}^{l} \frac{F_i^{\phi}(g)}{i!} f^i \quad \text{for } f, g \in k(X). \tag{3.4}$$

Now, we prove Proposition 2.2. Suppose to the contrary that there exists $\Phi \in L_{\Delta}^{\epsilon} \cap k[X]$ in which X_3^l appears for some $l \in \mathbf{N}$. By Proposition 3.2, Φ is contained in $k[\Pi] \cap k[X]$. By replacing Φ with its $\mathbf{Z}$-homogeneous component in which X_3^l appears, we may assume that Φ is in $V_{l\delta_0}$. Write $\Phi = \sum_{i \geqslant 0} (\phi_{l-i}/i!) \Pi_0^i$, where $\phi_i \in k[\Pi_1, \Pi_2]$ for each i. Then, we may assume that ϕ_i is in $V_{i\delta_0}$ for each i. Note that $k[\Pi_1, \Pi_2] \cap V_{i\delta_0}$ is equal to k if $i = 0$, and $\{0\}$ if $i = 1$ or $i < 0$. Indeed, Π_i is in V_{δ_i} for $i = 1, 2$, and $0 < \delta_0 < \delta_1 < \delta_2$ by the choice of δ_1 and δ_2. Hence, $\phi_0 = \alpha$ for some $\alpha \in k$ and $\phi_i = 0$ for $i = 1$ and $i < 0$. We remark that α is not zero, since X_3^l appears in Φ by assumption, but does not appear in $\phi_{l-i} \Pi_0^i$ for any $i \neq l$. Put $\phi = (\phi_i)_{i=0}^{l}$. Then, $\Phi = F_0^{\phi}(\Pi_0)$. Since $\Pi_0 = X_2^{-\delta_0} + X_3$, we have $\Phi = \sum_{i=0}^{l} (F_i^{\phi}(X_2^{-\delta_0})/i!) X_3^i$ by the formula (3.4). This implies that $F_i^{\phi}(X_2^{-\delta_0})$ is in $k[X]$ for each i, since Φ is in $k[X]$ and $F_i^{\phi}(X_2^{-\delta_0})$ does not involve X_3. In particular, $F_{l-1}^{\phi}(X_2^{-\delta_0}) = \phi_0 X_2^{-\delta_0} + \phi_1 = \alpha X_2^{-\delta_0}$ is in $k[X]$, a contradiction. Therefore, there does not exist $\Phi \in L_{\Delta}^{\epsilon} \cap k[X]$ in which X_3^l appears. This completes the proof of Proposition 2.2.

4. Construction of elements of $L_{\Delta}^{\epsilon} \cap k[X]$

Let $v : k(X) \to \mathbf{Z} \cup \{\infty\}$ be the X_2-adic valuation of $k(X)$ with $v(X_2) = 1$, i.e., $v(f) = r$ for $f \in k(X) \setminus \{0\}$ and $r \in \mathbf{Z}$ if $f = X_2^r f_1/f_2$ for some $f_1, f_2 \in k[X] \setminus X_2 k[X]$, and $v(0) = \infty$. Then, f is contained in $k[X]$ if and only if $v(f) \geqslant 0$ for $f \in k[X][X_2^{-1}]$. We remark that $v(\Pi_i) = -\delta_i$ and Π_i is in V_{δ_i} for $i = 0, 1, 2$. So, if $f \in k[\Pi]$ is contained in V_l for some $l \in \mathbf{Z}$, then $v(f) \geqslant -l$. We set $\hat{\Pi} = \Pi_1^{\delta_2'} - \Pi_2^{\delta_1'}$. Then, $\hat{\Pi} = X_2^{-\delta_0'}(\pi_1^{\delta_2'} - \pi_2^{\delta_1'})(X_1 X_2^{\epsilon})$. Since $\pi_1^{\delta_2'} - \pi_2^{\delta_1'}$ is in $z^{\epsilon'} k[z] \setminus z^{\epsilon'+1} k[z]$ by the choice of ϵ', we get $v((\pi_1^{\delta_2'} - \pi_2^{\delta_1'})(X_1 X_2^{\epsilon})) = \epsilon\epsilon'$. By assumption, $\epsilon\epsilon' \geqslant \delta_0' + 1$. Thus, we obtain that $v(\hat{\Pi}) \geqslant 1$. Note that there exist $q_1, q_2 \in \mathbf{N}$ such that $q_1\delta_1 = q_2\delta_2 + \delta_0$.

Indeed, δ_0 is the greatest common divisor of δ_1 and δ_2, and δ_2 is not divisible by δ_1. We set $\check{\Pi} = \Pi_1^{q_1}\Pi_2^{-q_2}$. Then,

$$X_2^{-\delta_0} - \check{\Pi} = X_2^{-\delta_0}\big(\Pi_2^{q_2} - X_2^{\delta_0}\Pi_1^{q_1}\big)\Pi_2^{-q_2} = X_2^{-\delta_0}\big(\pi_2^{q_2} - \pi_1^{q_1}\big)\big(X_1X_2^{\epsilon}\big)\pi_2\big(X_1X_2^{\epsilon}\big)^{-q_2}. \quad (4.1)$$

By assumption, $\pi_1(0) = \pi_2(0) = 1$, and so $\pi_2^{q_2} - \pi_1^{q_1}$ is contained in $zk[z]$. Hence, $v(\pi_2(X_1X_2^{\epsilon})) = 0$ and $v((\pi_2^{q_2} - \pi_1^{q_1})(X_1X_2^{\epsilon})) \geqslant \epsilon$. Thus, we get $v(X_2^{-\delta_0} - \check{\Pi}) \geqslant \epsilon - \delta_0 \geqslant 0$ by (4.1), since $\epsilon \geqslant \delta_0$ by assumption. As a consequence, we obtain that $v(\Pi_0 - \check{\Pi}) \geqslant 0$.

Lemma 4.1. *Let l and m be integers with $l \geqslant 0$ and $m \geqslant \delta_0' + 1$. Then, for each $\Phi \in k[\Pi_1, \Pi_2] \cap V_{lq_1\delta_1 + m\delta_0'}$, there exists $\phi \in k[\Pi_1, \Pi_2] \cap V_{l\delta_0 + m\delta_0'}$ such that $v(\Phi\Pi_2^{-lq_2} + \phi) \geqslant 0$.*

Proof. There exists an integer u with $0 \leqslant u < \delta_2'$ such that Φ is expressed as a linear combination of $\Pi_1^{(i_0-i)\delta_2'}\Pi_2^{i\delta_1'}$ for $i = 0, \ldots, i_0$ over k multiplied by Π_1^u, where $i_0 = (lq_1 - u)/\delta_2' + m$. Since $\Pi_1^{\delta_2'} = \hat{\Pi} + \Pi_2^{\delta_1'}$, we may write $\Phi = \Pi_1^u \sum_{i=0}^{i_0} \alpha_i \hat{\Pi}^{i_0-i}\Pi_2^{i\delta_1'}$, where $\alpha_i \in k$ for each i. Let i_1 be the minimal integer such that $i_1\delta_1' \geqslant lq_2$. We set

$$\phi = -\Pi_1^u \sum_{i=i_1}^{i_0} \alpha_i \hat{\Pi}^{i_0-i}\Pi_2^{i\delta_1' - lq_2} \quad \text{and} \quad \Phi_1 = \hat{\Pi}^{-(i_0-i_1+1)}\Pi_1^u \sum_{i=0}^{i_1-1} \alpha_i \hat{\Pi}^{i_0-i}\Pi_2^{i\delta_1' - lq_2}.$$

Then, $\Phi\Pi_2^{-lq_2} + \phi = \hat{\Pi}^{i_0-i_1+1}\Phi_1$. Put $d = l\delta_0 + m\delta_0' - (i_0 - i_1 + 1)\delta_0'$. Then, Φ_1 is contained in $k[\Pi_1, \Pi_2] \cap V_d$. Hence, $v(\Phi_1) \geqslant -d$ as mentioned. Thus, we get

$$v\big(\Phi\Pi_2^{-lq_2} + \phi\big) = (i_0 - i_1 + 1)v(\hat{\Pi}) + v(\Phi_1) \geqslant (i_0 - i_1 + 1)\big(1 + \delta_0'\big) - l\delta_0 - m\delta_0', \quad (4.2)$$

since $v(\hat{\Pi}) \geqslant 1$. By definition, $u < \delta_2'$ and $i_1 < lq_2/\delta_1' + 1$. So, we have

$$i_0 - i_1 > \left(\frac{lq_1}{\delta_2'} - \frac{u}{\delta_2'} + m\right) - \left(\frac{lq_2}{\delta_1'} + 1\right) > \frac{l(q_1\delta_1 - q_2\delta_2)}{\delta_1\delta_2'} + m - 2 = \frac{l\delta_0}{\delta_0'} + m - 2.$$

Besides, $l \geqslant 0$ and $m \geqslant \delta_0' + 1$ by assumption. Thus, the right-hand side of (4.2) is not less than

$$\left(\frac{l\delta_0}{\delta_0'} + m - 1\right)\big(1 + \delta_0'\big) - l\delta_0 - m\delta_0' = \left(\frac{l\delta_0}{\delta_0'} + m - 1\right) - \delta_0' \geqslant (m-1) - \delta_0' \geqslant 0.$$

Therefore, we obtain that $v(\Phi\Pi_2^{-lq_2} + \phi) \geqslant 0$. □

Take $m \in \mathbf{N}$ with $m \geqslant \delta_0' + 1$ and put $\phi_0 = \hat{\Pi}^m$. Note that ϕ_0 is an element of $V_{m\delta_0'}$.

Lemma 4.2. *For each $l \in \mathbf{Z}_{\geqslant 0}$, there exist $\phi_1, \ldots, \phi_l \in k[\Pi_1, \Pi_2]$ with $\phi_i \in V_{i\delta_0 + m\delta_0'}$ for each i such that $v(F_j^{\phi}(\check{\Pi})) \geqslant 0$ for $j = 0, \ldots, l$, where $\phi = (\phi_i)_{i=0}^{l}$.*

Proof. We show the lemma by induction on l. The assertion is clear when $l = 0$. Assume that there exist $\phi_1, \dots, \phi_{l-1} \in k[\Pi_1, \Pi_2]$ as claimed for some $l > 0$. Set $\Phi = \Pi_2^{lq_2} \sum_{i=1}^{l} \phi_{l-i} \check{\Pi}^i / i!$. Then, Φ is contained in $k[\Pi_1, \Pi_2] \cap V_{lq_1\delta_1 + m\delta_0'}$. By Lemma 4.1, there exists $\phi_l \in k[\Pi_1, \Pi_2] \cap V_{l\delta_0 + m\delta_0'}$ such that $v(\Phi \Pi_2^{-lq_2} + \phi_l) \geqslant 0$. Put $\phi = (\phi_i)_{i=0}^{l}$ and $\phi' = (\phi_i)_{i=0}^{l-1}$. Then, $v(F_0^{\phi}(\check{\Pi})) \geqslant 0$, since $F_0^{\phi}(\check{\Pi}) = \Phi \Pi_2^{-lq_2} + \phi_l$. By induction assumption, we have $v(F_i^{\phi'}(\check{\Pi})) \geqslant 0$ for $i = 0, \dots, l-1$. Since $F_i^{\phi}(\check{\Pi}) = F_{i-1}^{\phi'}(\check{\Pi})$, we get $v(F_i^{\phi}(\check{\Pi})) \geqslant 0$ for $i = 1, \dots, l$. Thus, $\phi_1, \dots, \phi_l$ satisfy the condition as claimed. Therefore, the assertion holds for any l. □

Now, let us prove Proposition 2.3. We show that there exists $\Phi_l \in L_{\Delta}^{\epsilon} \cap k[X]$ of the form $\Phi_l = (\phi_0 / l!) X_3^l +$ (terms of lower degree in X_3) for each $l \in \mathbf{N}$. Take $\phi_1, \dots, \phi_l \in k[\Pi_1, \Pi_2]$ as in Lemma 4.2, and define $\Phi_l = F_0^{\phi}(\Pi_0)$, where $\phi = (\phi_i)_{i=0}^{l}$. Then, $\Phi_l = \sum_{i=0}^{l} (F_i^{\phi}(X_2^{-\delta_0}) / i!) X_3^i$ by the formula (3.4), and $F_l^{\phi}(X_2^{-\delta_0}) = \phi_0$. Hence, Φ_l has this form. Clearly, Φ_l is an element of L_{Δ}^{ϵ}. So, it remains only to verify that Φ_l is contained in $k[X]$. By the formula (3.4), we have

$$\Phi_l = F_0^{\phi}(\check{\Pi} + \Pi_0 - \check{\Pi}) = \sum_{j=0}^{l} \frac{F_i^{\phi}(\check{\Pi})}{i!} (\Pi_0 - \check{\Pi})^i. \tag{4.3}$$

By the choice of $\phi_1, \dots, \phi_l$, we get $v(F_i^{\phi}(\check{\Pi})) \geqslant 0$ for each i. As mentioned before Lemma 4.1, $v(\Pi_0 - \check{\Pi}) \geqslant 0$. Thus, we obtain $v(\Phi_l) \geqslant 0$ by (4.3). Since Φ_l is in $k[X][X_2^{-1}]$, this implies that ϕ_l is contained in $k[X]$. Therefore, Φ_l is an element of $L_{\Delta}^{\epsilon} \cap k[X]$ of the form as claimed. This proves Proposition 2.3, and thereby completes the proof of Theorem 1.1.

5. Remarks

First, we show that $k(X)/L_{\Delta}^{\epsilon}$ is not a Galois extension for the Δ we discussed before Corollary 1.3. By Proposition 1.2, it suffices to verify that $k(X)'/M_{\Delta}$ is not a Galois extension.

Proposition 5.1. *The number of the automorphisms of $k(X)'$ over M_{Δ} is at most δ_0. In particular, $k(X)'/M_{\Delta}$ is not a Galois extension.*

Proof. Recall that $[k(X)' : M_{\Delta}] = \delta_2$ and $k(X)'$ is generated by X_2 over M_{Δ}. Since $\delta_2 > \delta_0$, the latter part follows from the former part. So, we prove the former part. Let ι be an automorphism of $k(X)'$ over M_{Δ}. Then, ι is uniquely determined by $\phi := X_2 / \iota(X_2)$. We show that ϕ is a δ_0th root of unity. Since $2X_2^{\delta_2} - \Pi_1' X_2^{\delta_2 - \delta_1} - \Pi_2' = 0$ as mentioned in Section 1, we have $2\iota(X_2)^{\delta_2} = \Pi_1' \iota(X_2)^{\delta_2 - \delta_1} + \Pi_2'$. From this equality, we get

$$2X_2 = \phi^{\delta_1}(X_2 - X_1) + \phi^{\delta_2}(X_2 + X_1) \tag{5.1}$$

by multiplying $\phi^{\delta_2} / X_2^{\delta_2 - 1}$ by its both sides and substituting X_2/ϕ for $\iota(X_2)$. Take mutually prime elements $\phi_1, \phi_2 \in k[X_1, X_2]$ with $\phi = \phi_1/\phi_2$. Then, (5.1) is written as

$$2X_2 \phi_2^{\delta_2} = \phi_1^{\delta_1} \big(\phi_2^{\delta_2 - \delta_1}(X_2 - X_1) + \phi_1^{\delta_2 - \delta_1}(X_2 + X_1) \big). \tag{5.2}$$

Since $\phi_2^{\delta_2}$ and $\phi_1^{\delta_1}$ are mutually prime, this implies that $\phi_1^{\delta_1}$ divides X_2. Hence, ϕ_1 must be an element of $k \setminus \{0\}$, since $\delta_1 > 1$. So, we may put $\phi_1 = 1$. Then, (5.2) is written as $\psi_2 X_2 = \psi_1 X_1$, where $\psi_1 = 1 - \phi_2^{\delta_2-\delta_1}$ and $\psi_2 = 2\phi_2^{\delta_2} - \phi_2^{\delta_2-\delta_1} - 1$. This implies that ϕ_2 is in k. Actually, if ϕ_2 is not in k and $\bar{\phi}_2$ is its highest degree part for the standard grading of $k[X_1, X_2]$, then $2\bar{\phi}_2^{\delta_2} X_2 = -\bar{\phi}_2^{\delta_2-\delta_1} X_1$. This is impossible, since $\delta_2 > \delta_2 - \delta_1$. Consequently, ψ_i is in k, and so $\psi_i = 0$ for $i = 1, 2$. These equalities imply $\phi_2^{\delta_i} = 1$ for $i = 1, 2$. Since δ_0 is the greatest common divisor of δ_1 and δ_2, it follows that ϕ is a δ_0th root of unity. Therefore, the number of the automorphisms of $k(X)'$ over M_Δ is at most δ_0. □

Next, we review the counterexample for $n = 3$ given in [6]. Let γ be a natural number and $\delta = (\delta_{i,j})_{i,j}$, where $\delta_{i,j} \in \mathbf{N}$ for each $i, j \in \{1, 2\}$ with

$$\frac{\delta_{1,1}}{\delta_{1,1} + \delta_{2,1}} + \frac{\delta_{2,2}}{\delta_{2,2} + \delta_{1,2}} < \frac{1}{2}. \tag{5.3}$$

For γ and δ, we define $L_{\gamma,\delta}$ to be the subfield of $k(X)$ generated by $F_1 := g_2 - g_1$, $F_2 := X_3^\gamma - g_1$ and $F_3 := 2g_1g_2 - g_1^2$ over k, where $g_1 = X_2^{\delta_{1,2}}/X_1^{\delta_{1,1}}$ and $g_2 = X_1^{\delta_{2,1}}/X_2^{\delta_{2,2}}$. We note that $L_{\gamma,\delta}$ is equal to the subfield of $k(X)$ generated by F_1, F_2 and g_2^2 over k, since $g_2^2 - F_3 = F_1^2$. Then, [6, Theorem 1.1] says that $L_{\gamma,\delta} \cap k[X]$ is not finitely generated. Let us show that

$$\big[k(X) : L_{\gamma,\delta}\big] = 2\gamma(\delta_{1,2}\delta_{2,1} - \delta_{1,1}\delta_{2,2}). \tag{5.4}$$

Put $M = k(g_1, g_2)$. Then, $M(X_3^\gamma)$ is not equal to $L_{\gamma,\delta}$, for otherwise M would be equal to $k(F_1, g_2^2)$. Moreover, $M(X_3^\gamma)$ is generated by g_1 over $L_{\gamma,\delta}$, and $g_1^2 + 2F_1g_1 - F_3 = 0$. Hence, we get $[M(X_3^\gamma) : L_{\gamma,\delta}] = 2$. It easily follows that $[M(X_3) : M(X_3^\gamma)] = \gamma$ and $[k(X) : M(X_3)] = [k(X)' : M]$. Furthermore, $[k(X)' : M] = \delta_{1,2}\delta_{2,1} - \delta_{1,1}\delta_{2,2}$. In fact, if $(a_{1,1}, a_{1,2})$ and $(a_{2,1}, a_{2,2})$ are linearly independent elements of $\mathbf{Z}^2$, then the extension degree of $k(X)'$ over its subfield generated by $X_1^{a_{i,1}} X_2^{a_{i,2}}$ for $i = 1, 2$ over k is equal to $|\det(a_{i,j})_{i,j}|$. Then, (5.4) follows from

$$\big[k(X) : L_{\gamma,\delta}\big] = \big[k(X) : M(X_3)\big]\big[M(X_3) : M\big(X_3^\gamma\big)\big]\big[M\big(X_3^\gamma\big) : L_{\gamma,\delta}\big].$$

For example, $\delta_{1,1} = \delta_{2,2} = 1$, $\delta_{1,2} = 3$ and $\delta_{2,1} = 4$ satisfy (5.3). In this case, $\delta_{1,2}\delta_{2,1} - \delta_{1,1}\delta_{2,2} = 11$, and so $[k(X) : L_{\gamma,\delta}] = 22\gamma$. We show that $\delta_{1,2}\delta_{2,1} - \delta_{1,1}\delta_{2,2} \geqslant 11$ whenever $\delta_{i,j}$'s satisfy (5.3). First, note that $\delta_{i,1} + \delta_{i,2} \geqslant 3$ for each i, for otherwise $\delta_{i,1} = \delta_{i,2} = 1$ for some i, and then (5.3) would not be satisfied. It also follows from (5.3) that $(\delta_{1,1} + \delta_{2,1})(\delta_{2,2} + \delta_{1,2}) < 2(\delta_{1,2}\delta_{2,1} - \delta_{1,1}\delta_{2,2})$. Hence, if $\delta_{1,2}\delta_{2,1} - \delta_{1,1}\delta_{2,2} < 11$, then $(\delta_{1,1} + \delta_{2,1})(\delta_{2,2} + \delta_{1,2}) < 20$. Due to symmetry, we may assume that $(\delta_{1,1} + \delta_{2,1}, \delta_{2,2} + \delta_{1,2})$ is one of $(3, 3)$, $(3, 4)$, $(3, 5)$, $(3, 6)$ and $(4, 4)$. In each case, the left-hand side of (5.3) is not less than $1/2$. This is a contradiction. Thus, $\delta_{1,2}\delta_{2,1} - \delta_{1,1}\delta_{2,2} \geqslant 11$. Therefore, $[k(X) : L_{\gamma,\delta}]$ can only be an even number at least equal to twenty-two.

References

[1] D. Daigle, G. Freudenburg, A counterexample to Hilbert's fourteenth problem in dimension 5, J. Algebra 221 (1999) 528–535.

[2] G. Freudenburg, A counterexample to Hilbert's fourteenth problem in dimension six, Transform. Groups 5 (2000) 61–71.

[3] H. Kojima, M. Miyanishi, On Roberts' counterexample to the fourteenth problem of Hilbert, J. Pure Appl. Algebra 122 (1997) 277–292.
[4] S. Kuroda, A generalization of Roberts' counterexample to the fourteenth problem of Hilbert, Tohoku Math. J. 56 (2004) 501–522.
[5] S. Kuroda, A counterexample to the Fourteenth Problem of Hilbert in dimension four, J. Algebra 279 (2004) 126–134.
[6] S. Kuroda, A counterexample to the Fourteenth Problem of Hilbert in dimension three, Michigan Math. J. 53 (2005) 123–132.
[7] S. Kuroda, Hilbert's Fourteenth Problem and invariant fields of finite groups, preprint.
[8] S. Mukai, Counterexample to Hilbert's fourteenth problem for the 3-dimensional additive group, preprint 1343, Research Institute for Mathematical Sciences, Kyoto University, 2001.
[9] M. Nagata, On the fourteenth problem of Hilbert, in: Proceedings of the International Congress of Mathematicians, 1958, Cambridge Univ. Press, London, 1960, pp. 459–462.
[10] E. Noether, Der Endlichkeitssatz der Invarianten endlicher Gruppen, Math. Ann. 77 (1916) 89–92.
[11] P. Roberts, An infinitely generated symbolic blow-up in a power series ring and a new counterexample to Hilbert's fourteenth problem, J. Algebra 132 (1990) 461–473.
[12] R. Steinberg, Nagata's example, in: Algebraic Groups and Lie Groups, in: Austral. Math. Soc. Lect. Ser., vol. 9, Cambridge Univ. Press, 1997, pp. 375–384.
[13] O. Zariski, Interprétations algébrico-géométriques du quatorzième problème de Hilbert, Bull. Sci. Math. 78 (1954) 155–168.